

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

03/13/2014

**SUBJECT:**

Vulnerability in Adobe Shockwave Player Could Allow for Remote Code Execution (APSB14-10)

**EXECUTIVE SUMMARY:**

A vulnerability has been discovered in Adobe Shockwave that could allow an attacker to remotely take control of the affected system. Adobe Shockwave is a multimedia platform used to add animation and interactivity to web pages. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

**THREAT INTELLIGENCE:**

At this time this vulnerability is not publicly disclosed and there is no known proof-of-concept code available.

**SYSTEMS AFFECTED:**

- Adobe Shockwave 12.0.9.149 and earlier

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**TECHNICAL SUMMARY:**

Adobe has released a security update for Adobe Shockwave Player 12.0.9.149 and earlier versions on the Windows and Macintosh operating systems. This update addresses a critical memory corruption vulnerability that could potentially allow an attacker to remotely take control of the affected system. An attacker could exploit this vulnerability by creating a web site that contains specially crafted content designed to exploit this vulnerability. Adobe recommends users of Adobe Shockwave Player 12.0.9.149 and earlier versions update to Adobe Shockwave Player 12.1.0.150.

**RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

**REFERENCES:****Adobe:**

<http://helpx.adobe.com/security/products/shockwave/apsb14-10.html>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0505>

**Security Focus:**

<http://www.securityfocus.com/bid/66182>